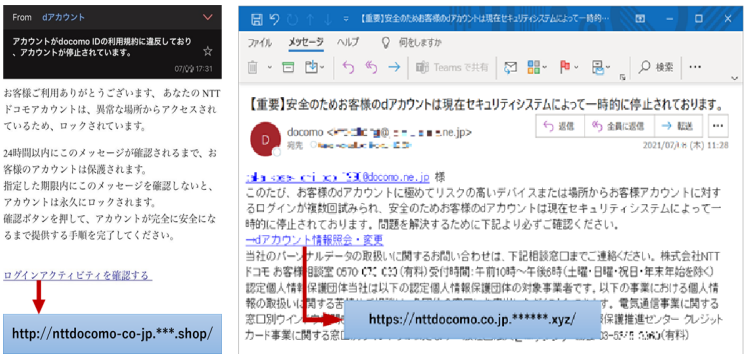
通信事業者を装った フィッシングに要注意！

電子メールやＳＭＳ（ショーメッセージサービス）を利用して、通信事業者を装ったフィッシングの手口が増加しています。

～確認されているフィッシングの手口～

○　フィッシングメール／ＳＭＳの送信元が偽装されている。
○　利用者の不安をあおり、早急に確認するよう促す内容がある。
○　運送系企業を装ったフィッシングメール／ＳＭＳから、通信事業者のフィッシングサイトへ誘導される場合がある。

【電子メールの例】



【SMSの例】

ドコモお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。
https://bit.[redacted]

～被害に遭わないために～

■　電子メールやＳＭＳのメッセージに含まれているリンク先を安易にクリックしないこと。
■　通信事業者からの通知内容を確認するときは、公式サイトから確認すること。
■　ＩＤ・パスワードを入力する際は、公式サイトであることを確認した上で入力すること。

今後も、色々な文面（文章）で、悪質なフィッシングサイトに誘導されて、個人情報が盗み取られることが懸念されますので、フィッシングメール／ＳＭＳに注意してください。

※出典：一般財団法人日本サイバー犯罪対策センター

【お問い合わせ先】
高知県警察本部生活安全部サイバー犯罪対策課　TEL088-826-0110